UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,255	06/28/2001	Sherry Chu-Hsin Hsu	50P4299.01/1575	9177

24272 7590 01/24/2006

Gregory J. Koerner
Redwood Patent Law
1291 East Hillsdale Boulevard
Suite 205
Foster City, CA 94404

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/896,255	HSU ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: amendment filed 29 September 2005, with an original application filed 28 June 2001, with acknowledgement of continuing filing date of 7 December 2000.

2. Claims 1-42 are currently pending in this application. Claims 1, 21, 41, and 42 are independent claims. Claims 1 and 21 have been amended.

3. Amendments to the claims are accepted.

Response to Arguments

4. Applicant's arguments with respect to claims 1-42 have been considered but have not been found persuasive.

In response to applicant's argument beginning on page 11, "For example, claim 1 is now amended to recite "said DMA engine including an encryption module that utilizes command information from said encryption structure and control information from said control registers for processing source data to produce destination data during said data encryption operation" (emphasis added), which are limitation that are not taught or suggest by the cited reference". The Office disagrees with the argument, the reference teaches that the DMA engine includes an encryption module see col. 7, line 35 through col. 8, line 43. This section explains that the DMA engine is both coupled to the input/output section, which can incorporate the cryptographic co-processor.

In response to applicant's argument on 12, "Applicants submit that column 2, lines 19-48 of Ober fails to disclose a processor creating an encryption structure as in claims 1 and 21". The Office disagrees with argument see col. 7, lines 23-34 which indicates "a microprocessor

forming part of the co-processor, which accesses the library and retrieves the particular encryption algorithm". The microprocessor is creating the encryption structure by selecting the encrypting algorithm.

In response to applicant's argument on page 12, "Applicants submit that Ober nowhere teaches or suggest a DMA engine including an encryption module". The Office disagrees with argument as stated above see col. 7, line 35 through col. 8, line 43.

In response to applicant's argument on page 13, "Applicants respectfully submit that, in light of the substantial differences between the teaching of Ober and Applicants' invention as disclosed in the Specification, claim 41 is therefore not anticipated or made obvious by the teaching of Ober". The Office disagrees with argument and notes that the only substantial difference between Ober and the claimed invention is that the applicant's specification is shorter.

In response to applicant's argument on page 13, "Applicants submit that column 25, lines 35-41 of Ober fails to disclose a "next command structure pointer" or a "control status command", as recited in claims 8 and 28". The Office disagree with argument see col. 31, line 52 through col. 32, line 67 which describes the DMA Status/Configuration Registers.

In response to applicant's argument beginning on page 13, "Applicants find no mention of the claimed elements of their "control status command". The Office disagree with argument the tables include command registers as well as interface registers which provide status and allow interrupts.

In response to applicant's argument on page 14, "Applicants submit that column 5, line 41 through col. 6, line 33 of Ober fails to disclose command structures that are linked together in a linked list, as recited in claims 10 and 30". The Office disagrees with argument, Ober shows

that multiple encryption algorithms are available and that these encryption operations an be linked so that they are performed at the same time or parallel execution which is interpreted to have the same meaning as a 'linked list'.

In response to applicant's argument on page 14, "Ober therefore fails to disclose that "said DMA engine includes a state machine for controlling said data encryption operation, or more command registers for locally storing one or more command structures from said encryption structure". The Office disagrees with argument Ober teaches the state machine is interpreted to be the DMA controller circuit see col. 4, lines 50-54.

In response to applicant's argument on page 14, "Applicants find no mention of the claimed elements of their "control status command" in either claim 1 or tables 1 & 2 of Ober". The Office disagrees with argument as stated previously the tables include command registers as well as interface registers which provide status and allow interrupts.

In response to applicant's argument on page 16, "Applicants also submit that neither Ober nor Okaue contain teaching for combing the cited references to produce the Applicants' claimed invention". The Office disagree with argument the motivation to combine as recited in the Office Action within Okaue col. 2, lines 57-61. In addition see Ober col. 1, lines 32 et seq. "Digital signal processors (DSPs) are widely used in devices such as modems, cellular telephones and facsimiles. With an increase in digital communications, data transmission security has become an issue in numerous DSP applications. A standard DSP is not capable of providing data transmission security; thus, additional hardware and software are required". A cellular telephone could be classified as a "digital electronics".

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

4. **Claims 1-3, 5-24, and 26-42** are rejected under 35 U.S.C. 102(e) as being anticipated by Ober et al. U.S. Patent No. 6,708,273 (hereinafter '273).

As to independent claim 21, "A method for performing a data encryption operation in an electronic system, comprising: creating an encryption structure in a memory device by utilizing a processor" is taught in '273 col. 2, lines 19-48 and col. 7, lines 23-34;

"programming control registers with said processor to perform said data encryption operation" is shown in '273 col. 5, lines 54-63;

"accessing said encryption structure and said control registers with a DMA engine; and" is disclosed in '273 col. 4, lines 46-60;

"processing source data with an encryption module of said DMA engine to produce destination data, said encryption module utilizing command information from said encryption structure and control information from said control registers to perform said data encryption operation" is taught in '273 col. 9, lines 36-67 and col. 7, line 35 through col. 8, line 43.

As to dependent claim 22, "wherein said data encryption operation includes at least one of a data encryption process and a data decryption process" is shown in '273 col. 2, lines 32-47.

As to dependent claim 23, "wherein said memory device receives said source data from a source entity coupled to said electronic system, said memory device responsively storing said source data into a source data memory location until said encryption module requires said source data to perform said data encryption operation" is disclosed in '273 col. 11, lines 7-43.

As to dependent claim 25, "wherein said electronic system includes a bridge device that facilitates bi-directional communications between said processor, one or more peripheral devices, said DMA engine, said encryption module, and said memory device" is shown in '273 col. 11, lines 1-43.

As to dependent claim 26, "wherein said bridge device includes a processor interface for communicating with said processor, a memory interface for communicating with said memory device, and one or more peripheral interfaces for communicating with said one or more peripheral devices" is disclosed in '273 col. 11, lines 32-43.

As to dependent claim 27, "wherein said encryption structure includes at least one command structure that has command information for performing said data encryption operation" is taught in '273 in col. 6, line 66 through col. 7, line 23.

As to dependent claim 28, "wherein said command structure includes a starting source address, a starting destination address, a transfer-bytes total field, a next command-structure pointer, and a control status command" is shown in '273 col. 25, lines 35-41.

As to dependent claim 29, "wherein said control status command includes an encryption/decryption field to indicate whether to perform one of said encryption process and said decryption process, an enabled/disabled field to indicate whether said data encryption operation is currently enabled, an interrupt field to designate whether an interrupt should occur following said data encryption operation, a last command field to indicate a final command structure in a linked list, and a transfer path identifier to indicate a source entity for said source data and a destination entity for destination data" is disclosed in '273 in tables 1 & 2, as well as claim 1.

As to dependent claim 30, "wherein said encryption structure includes a series of command structures that are linked together in a linked list to thereby perform a series of data encryption operations" is taught in '273 col. 5, line 41 through col. 6, line 33.

As to dependent claim 31, "wherein said DMA engine includes a state machine for controlling said data encryption operation, one or more command registers for locally storing one or more command structures from said encryption structure, said control registers, a data buffer, an encryption key register, and said encryption module" is shown in '273 col. 5, line 41 through col. 6, line 33.

As to dependent claim 32, "wherein said control registers include a start register that said processor may program to start said data encryption operation, a halt/resume register that said processor may program to halt or resume said data encryption operation, a clear interrupt register that said processor may program to clear an interrupt of said data encryption operation, a link list address register that said processor may program with a physical address in said memory device of a first command structure in said

encryption structure, and a status register that said DMA engine may program to indicate a current status of said data encryption operation" is disclosed in '273 in tables 1 & 2, as well as claim 1.

As to dependent claim 33, "wherein said processor initially creates said encryption structure in said memory device, said encryption structure including one or more command structures that each include command information for performing a separate data encryption operation" is taught in '273 col. 7, lines 23-52.

As to dependent claim 34, "wherein said processor programs said control registers with data encryption information that is then locally available to said DMA engine for performing said data encryption operation" is shown in '273 col. 7, lines 23-52.

As to dependent claim 35, "wherein said processor instructs said DMA engine to perform said data encryption operation after programming said control registers, said processor then releasing control of said data encryption operation and performing other system processing tasks for said electronic system" is disclosed in '273 col. 7, lines 44-67.

As to dependent claim 36, "wherein said DMA engine copies one or more designated command structures from said encryption structure in said memory device into one or more command registers that are locally coupled to said DMA engine" is taught in '273 col. 7, line 65 through col. 8, line 23.

As to dependent claim 37, "wherein said DMA engine controls said data encryption operation by referring to said control registers and said command registers" is shown in '273 col. 11, lines 14-24.

As to dependent claim 38, "wherein a state machine coupled to said DMA engine transfers said source data from said memory device to a data buffer coupled to said encryption module, said encryption module responsively performing at least one of said data encryption process and said data decryption process to produce said destination data, said state machine then storing said destination data back into said memory device" is disclosed in '273 col. 11, lines 1-24.

As to dependent claim 39, "wherein said DMA engine detects a completion condition while performing said data encryption operation, said DMA engine responsively notifying said processor regarding said completion condition" is taught in '273 col. 7, lines 43-52.

As to dependent claim 40, "wherein said processor transfers said destination data from said memory device to a destination entity that is coupled to said electronic system" is shown in '273 col. 7, lines 65 through col. 8, line 55.

As to independent claim 1, this claim is directed to an apparatus performing the method of claim 21 therefore it is rejected along similar rationale.

As to dependent claims 2-3; these claims are substantially similar to dependent claims 22 and 23; therefore they are rejected along similar rationale.

As to dependent claims 5-20, these claims contain substantially similar subject matter as claims 25-40; therefore they are rejected along similar rationale.

As to independent claim 41, this claim is directed to the apparatus for performing the method of claim 21 therefore it is rejected along similar rationale.

As to independent claim 42, this claim is directed to an apparatus for performing a data processing operation of the method of claim 21 therefore it is rejected along similar rationale.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 4 and 24** are rejected under 35 U.S.C. 103(a) as being unpatentable over '273 in further view of Okaue et al. U.S. Patent No. 6,820,203 (hereinafter '203).

As to dependent claim 24, the following is not taught in '273 **"wherein said electronic system is implemented as one of an audio/visual electronic device, a consumer electronics device, a portable electronics device, and a computer device"** however '203 teaches "The security unit is particularly useful as part of a memory unit that is attachable to a recording/reproduction device such as a digital audio recorder/player" in col. 2, lines 57-61.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '273 a secure communication platform on an integrated circuit which incorporates a high performance cryptographic function to include a means to send information to an audio/visual portable device. One in the art would have been motivated to perform such a

modification to maintain security on a small circuit scale (see '273 col. 2 lines 28-48) "Accordingly, a memory card with an internal security unit may be provided with two types of registers: an accessible register for storing data to be transferred to the set in response to a command requesting the same; and a non-accessible register for storing an intermediate calculation result of the encryption process. Consequently, with two registers, the circuit scale of the security unit becomes large. This hampers the ability to increase the integration of the security unit structured as an IC chip. When the encryption process is to be performed a number of times, in order to remove a register that temporarily stores data, it is necessary to employ a plurality of encryption circuits so as to obtain all final data (encrypted data) at about the same time. Thus, in this case, the circuit scale also increases ... Accordingly, an object of the present invention is to provide a security unit that allows security to be maintained in a small circuit scale. Another object of the invention is to provide a memory unit that includes a security unit with a small circuit scale".

As to dependent claim 4, this claim contains substantially similar subject matter as claim 24; therefore it is are rejected along similar rationale.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened

statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen. Tran
Patent Examiner
Technology Center 2134
20 January 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100